

Net-Sec newsletter
Issue 30 - 18.09.2000
<http://net-security.org>

Net-Sec is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://www.net-security.org>.

Subscribe to this weekly digest on:
<http://www.net-security.org/text/newsletter>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured articles
- 5) Security books
- 6) Security software
- 7) Defaced archives

=====
Sponsored by VeriSign - The Internet Trust Company
=====
Do you use the Internet to deliver the software you develop?
Get VeriSign's FREE Guide to learn how you can digitally "shrink-wrap" your code to protect it against tampering, and how to sign your ActiveX controls, .cab files, jar files, HTML content, VB code, or Microsoft Office 2000 .doc files with a VeriSign Software Developer Digital ID.
Go to:
<http://www.verisign.com/cgi-bin/go.cgi?a=n037010570200000>
=====

General security news

WORLD OF SPIES GETS PORTAL

While the secrets of the Russian secret services aren't likely to be made available to the general public anytime soon, a curious person can now turn to a new Internet portal, www.agentura.ru, to make basic inroads into the murky world of spies. "We're counting on the big existing interest in this topic and we want to fill in the information vacuum," said Andrei Soldatov, a political journalist with the influential Izvestia daily, who together with his father - Alexei Soldatov, president of the Relcom Internet provider - started the portal.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.themoscowtimes.com/stories/2000/09/14/010.html>

MORE ON CARNIVORE

Several prominent universities have rejected the U.S. Justice Department's appeal to universities to test an electronic eavesdropping device known as Carnivore. Researchers from four universities have complained that the department has too much control over the review, and their public comments have prompted a fifth university to ignore the department's request.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://chronicle.com/free/2000/09/2000091501t.htm>

720 WEB SITES DEFACED

Some of the sites remain defaced early Monday morning, with an anti-racism message left by the hacker, who calls him or herself "piffy." Piffy belongs to a group known as the RootShellHackers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/pubNews/00/155311.html>

INTRODUCTION TO ENCRYPTION

Joshua Ryder did a good job with this introductory article. It goes from the very basics of explaining what encryption is ("Encryption is the process of converting data from one form into ciphertext"), and goes along with some basic examples of how encryption works.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/cover/coverstory20000918.html>

A FEW RECIPES FOR EASIER FIREWALLS

"Every day, we hear of damage caused by viruses, of new exploits through which crackers compromise systems. For those of us in the information technology restaurant business, these are challenging times. We must be ever vigilant. A good firewall, then, is an excellent beginning. But how to do it simply is the question..."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/lj-issues/issue78/4218.html>

QAZ.TROJAN

This new backdoor Trojan allows attackers to access and control an infected system. TROJ_QAZ was initially distributed as "Notepad.exe" but might also appear with different filenames. Once an infected file is executed, TROJ_QAZ modifies the Windows registry so that it becomes active every time Windows is started. TROJ_QAZ also renames the original "notepad.exe" file to "note.com" and then copies itself as "notepad.exe" to the Windows folder. This way, the Trojan is also launched every time a user runs Notepad. TROJ_QAZ also attempts to spread itself to other shared drives on local networks.

Link: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_QAZ.A

MASSIVE DDOS?

Attackers are using the rcp.statd and wu-ftpd vulnerabilities to ready another distributed Denial of Service attack. MSNBC is reporting there are at least 560 computers infected.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://slashdot.org/articles/00/09/16/215225.shtml>

SMARTCARDS BENEFIT FROM BIOMETRICS

Fingerprint authentication specialist Veridicom has announced a new combined smartcard reader and fingerprint scanner that is designed to improve smartcard authentication systems by replacing passwords with biometric security. Analyst firm Gartner Group recently reported that each year firms spend \$350 per user managing password issues.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/37/ns-17927.html>

AUTHOR OF CIH VIRUS ARRESTED IN TAIWAN

The virus writer who created the infamous Chernobyl virus has been detained by authorities in Taiwan and could face up to 3 years in jail.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/36/ns-17921.html>

AN INTERVIEW WITH PIMPSHIZ

"I met pimpshiz in the time span that Observers has been up, sometime in the last two years, when the news reports broke about "pimpshiz" having been responsible for the widespread defacement of websites in a protest over the potential closing of Napster. I wondered if it was the same individual we here at observers knew, and to my shock it was."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.observers.net/pimpshiz.html>

EXPLOITATION OF RCP.STATD AND WU-FTPD VULNERABILITIES

Sites involved in related incidents are reporting finding hosts compromised through one of these two vulnerabilities. In several cases, hundreds of compromised hosts have been involved in single incidents. Intruders appear to be using automated tools to probe for and exploit vulnerable hosts on a widespread scale. A large majority of the compromised hosts involved in this activity have been running various versions of Red Hat Linux. Insecure default configurations in some versions, especially with respect to the vulnerable rpc.statd service often being enabled during automated installation and upgrade processes, have contributed to the widespread success of these attacks.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/incident_notes/IN-2000-10.html

PGP "UNHASHED SUBPACKET" PROBLEM - SERIOUS?

"I've been studying the UNIX source code for PGP 6.5.1i, and it seems to me that the "unauthorized ADK" bug could be just one manifestation of what may in fact be a far more serious problem. As best I can tell, PGP's that implement the new (version-4) data format do not appear to care whether ANY signature subpacket is in the hashed section of the signature or not. If I'm right, the signature hashing mechanism can be bypassed completely, and ANY info in ANY version-4 signature (not just ARR/ADK info) can be easily forged by a malicious attacker."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/pgp-badbug2.htm>

SECURITY SCANNERS

"There are various tools available for Linux system scanning and intrusion detection. I will explain some of the very famous tools available. I have divided the scanners into three categories: Host Scanners, Network Scanners, and Intrusion Scanners."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://linuxsecurity.com/feature_stories/feature_story-66.html

LINUX COMMUNITY SNUBS SDMI HACKER CHALLENGE

The Linux Journal is sponsoring a boycott of the Secure Digital Music Initiative hacking challenge, which promises to pay \$10,000 to any hacker who strips out the watermark from a digital song. Some Linux lovers say the record industry is using the hackers as a "free consulting" service to help it crack down on legal uses of music in the future, in an attempt to exert unprecedented control over when and where people play songs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/36/ns-17904.html>

REPORTS RAISE QUESTIONS OVER WEB SECURITY

Fresh doubt has been cast on the security of using the Internet for commercial purposes after several high-profile Web sites were targeted by attackers. Two separate reports say that while consumers may prefer to use e-mail rather than the telephone, inefficient and insecure systems mean they often have to resort to the telephone anyway.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/09/14/britain.websecurity/index.html>

MICHIGAN "ANTI-HACKER" LAW'S FIRST FELONY CHARGES

Attorney General Jennifer Granholm today announced that she has filed felony criminal charges against two Michigan men each accused of unlawfully entering a third-party computer system. The charges are the first under a Michigan law which makes the unauthorized alteration, damage or use of a computer system a felony.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ag.state.mi.us/AGWebSite/press_release/pr10189.htm

HACKER SUED BY AN ANTITERRORIST JUDGE

Vincent Plousey aka Larsen, who's been arrested by the DST (french counter-

intelligence agency), is accused of having disclosed national defence secrets by an antiterrorist judge. The trouble is that the informations he revealed on the Net are freely available in bookshops...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/larsen091200.htm>

NEW TECHNOLOGY TRACKS, KILLS DOS ATTACKS AT ISP LEVEL

With the DoS attacks on the rise, four University of Washington computer networking experts formed a company, called Asta Networks, aimed at protecting websites from assaults. Stefan Savage, a Ph.D. candidate whose research is at the center of Asta's technology, said he and his computer science advisors decided they could have a greater impact on the industry by forming a company rather than by writing papers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.planetit.com/techcenters/docs/security/news/PIT20000914S0028>

ONLINE FRAUDSTERS FLEECE UK ETAILERS

Online crime pays, according to a report published today by Experian. The global information solutions group claims nine out of ten efraudsters aren't caught and are simply getting away with it. The survey reveals that when it comes to checking the authenticity of credit card transactions, many of Britain's etailers are lax. The survey of 800 British etailers found that many online authentication systems were wanting and most relied on manual systems to check credit card details.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/13251.html>

COME MEET THE SUSE LINUX SECURITY TEAM

Meet the guys who repair and document security flaws for SuSE in this brief article. Further down the same page you'll find security reports, updates and resources.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.lwn.net/2000/0914/security.php3>

E-SIGNATURE ACT

Some deals are still done with a signature on the dotted line, even with the advent of the Net. San Francisco-based LeaseExchange can process a rental request in less than a minute, but it can take days to execute leases – that is, getting everyone to sign the paperwork. CEO Aaron Ross admits it's "a very inefficient process right now." He's eager to see whether authentication technologies will speed things up without harming customer relationships.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/09/12/esigs.drive.demand.idg/index.html>

EVE.COM SECURITY BREACH

San Francisco Bay Area software developer Jonathan Khoo, discovered a breach in Eve.com, that allowed customers to view other people's orders by simply changing a number in the URL. After that, Eve.com shut down their servers, and now they are back online again.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1007-200-2770505.html>

SEVERAL TAIWANESE SITES PENETRATED

Several Taiwanese electronic newspapers and Web newsletters published by IT companies were broken into Tuesday by a hacker presumed to be based in China.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://asia.internet.com/2000/9/1303-taiwan.html>

HARRIS INTERACTIVE DROPS ITS LAWSUIT

Major polling firm Harris Interactive has dropped its lawsuit against Microsoft

Corp., Qwest Communications International Inc., America Online Inc. and other ISPs it accused of unfairly blocking its e-mail. Along with the ISPs, Harris also sued the Mail Abuse Prevention System, which put Harris on its "black hole" list of spammers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com>

VISA SEEKS NET SECURITY WITH "SMART CARD"

In a bid to provide tighter security for e-commerce and other transactions, Visa U.S.A. rolled out its new digital-based "smart card" on Tuesday. The smart card will store customer identification and account information within a microprocessor chip, and only smart card readers will be able to access the secured data.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ecommercetimes.com/news/articles2000/000913-4.shtml>

=====
==

Sponsored by Dialego - Online Market Research

=====
==

We conduct the first world-wide online survey for IT-security specialists. Please click http://www.dialego.de/1033_it/_e/sman.php3?co=e , fill in the online questionnaire and you may be one of the lucky people to win prizes in the amount of altogether € [EURO] 1500:

1st prize: Casio Digital Camera

2nd prize: 3Com Palm Personal Digital Assistant

3rd prize: Tandem parachute jump

plus 50 personal firewalls as individual protection for your computer plus 50 programs for boot protection and hard disk encryption

=====
==

Security issues

All vulnerabilities are located at:
<http://net-security.org/text/bugs>

WEBSHERE APPLICATION SERVER PLUGIN ISSUE

WebSphere uses the HTTP Host: header to decide which WAS Virtual Host will service a particular request. If you send huge amounts of data in the Host: request header. Depending on how many bytes were in the Host: header, you could cause the web server process to fault on either signal 11 (SIGSEGV) or signal 10 (SIGBUS).

Link: <http://www.net-security.org/text/bugs/969275035,75755,.shtml>

INTERNET SHOPPER'S MAIL SERVER OPEN RELAY BUG

Internet Shopper Ltd's Mail Server can be made to accept and handle mail for non-local sites. The version involved is Internet Shopper Ltd's Mail Server v3.02.13

Exploit: The use of the semi-colon in the "mail from" command will allow mail to be sent to machine that aren't local.

Link: <http://www.net-security.org/text/bugs/969274960,45311,.shtml>

MDAEMON WEB SERVICES HEAP OVERFLOW DoS

The Mdaemon Worldclient on TCP port 3000 and the Mdaemon Webconfig on TCP port 3001 both contain the same vulnerability. If a certain request is sent to the web service, it results in a heap overflow, crashing the service with a Dr. Watson access violation. This appears to be a general problem in the way that Mdaemon handles these kinds of URLs, so if other Mdaemon web services are used, those are probably vulnerable as well. The reason that the before mentioned services were tested is that they are enabled in a default installation.

Link: <http://www.net-security.org/text/bugs/969274876,97962,.shtml>

VULNERABILITY IN CAMSHOT SERVER

CamShot is a web server that serves up web pages containing time stamped images captured from a video camera. This product contains a remotely exploitable security vulnerability that allows a remote attacker to gain elevated privileges on the remote system.

Link: <http://www.net-security.org/text/bugs/969156843,52782,.shtml>

MICROSOFT'S NTLM PATCH RE-RELEASED

Microsoft has released a patch that eliminates a security vulnerability in the telnet client that ships with Microsoft(r) Windows 2000. The vulnerability could, under certain circumstances, allow a malicious user to obtain cryptographically protected logon credentials from another user.

Link: <http://www.net-security.org/text/bugs/969156774,38080,.shtml>

SAMBAR SERVER SEARCH CGI VULNERABILITY

The vulnerability occurs in the search.dll Sambar ISAPI Search shipped with this product. This dynamic link loader does not check on the 'query' parameter that is parsed to the server, therefore by constructing a malformed URL we are able to view the contents of the server, all folders, and files.

Link: <http://www.net-security.org/text/bugs/969156650,43479,.shtml>

RED HAT LINUX - FORMAT STRING EXPLOIT IN SCREEN

Screen allows the user to overload the visual bell with a text message that can be set by the user. This text message is handled as a format string, instead of as a pure string, so maliciously written format strings are allowed to overwrite the stack. Since screen in Red Hat Linux 5.2 and earlier releases was setuid root, this security hole could be exploited to gain a root shell.

Link: <http://www.net-security.org/text/bugs/968981154,31859,.shtml>

SLACKWARE LINUX - XCHAT INPUT VALIDATION BUG FIXED

An input validation bug was found to affect Slackware Linux 7.0, 7.1, and -current. The problem is described in detail here:

<http://www.securityfocus.com/bid/1601>

Users of Slackware 7.0, 7.1, and -current are urged to upgraded to the xchat.tgz package available in the Slackware -current branch.
Link: <http://www.net-security.org/text/bugs/968981067,67750,.shtml>

LINUX MANDRAKE - MOD_PHP3 UPDATE

A problem exists with PHP3 and PHP4 scripts regarding RFC 1867-based file uploads. PHP saves uploaded files in a temporary directory on the server, using a temporary name that is referenced as the variable \$FOO where "FOO" is the name of the file input tag in the submitted form. Many PHP scripts process \$FOO without taking measures to ensure that it is in fact a file that resides in the temporary directory. Because of this, it is possible for a remote attacker to supply an arbitrary file name as the value for \$FOO by submitting a standard form input tag by that name, and thus cause the PHP script to process arbitrary files. The vulnerability exists in various scripts, and not necessarily with PHP itself, as the script determines what actions to perform on the uploaded file.
Link: <http://www.net-security.org/text/bugs/968980963,39268,.shtml>

Security world

All press releases are located at:
<http://net-security.org/text/press>

CHEK POINT ANNOUNCES SECURE VIRTUAL NETWORK - [13.09.2000]

Check Point Software Technologies, the worldwide leader in securing the Internet, announced Secure Virtual Network (SVN) Solution Pack for Startups, bringing enterprise-class security to new Internet businesses. SVN Solution Pack for Startups is an affordable, integrated security solution that provides startup companies with the manageability, reliability, and scalability they need to secure their growing eBusinesses today and into the future.

Press release:
< <http://www.net-security.org/text/press/968677302,82000,.shtml> >

ACCORD NETWORKS ANNOUNCES VIDEO FIREWALL GATEWAY - [13.09.2000]

Accord Networks, the leading manufacturer of a family of IP, ATM, and ISDN visual and voice communications solutions including network switches, conference bridges, gateways and management systems, announced the Accord(R) V2GC-20 Firewall Gateway, the latest member of the Accord V2IPERA family of advanced IP video and voice products and services.

Press release:
< <http://www.net-security.org/text/press/968677453,73167,.shtml> >

AXENT'S RAPTOR FIREWALL "STILL FIRED UP" - [13.09.2000]

AXENT Technologies, Inc., one of the world's leading Internet security solution providers for e-business, that recently entered into a definitive agreement with Symantec Corporation to be acquired, announced today that its market-leading perimeter security solution, Raptor Firewall, was praised as "still fired up" in a recent InternetWeek magazine review for its proxy-based security, improved management console and integrated virtual private network (VPN) solution. The reviewer commended Raptor Firewall for its interoperability and flexibility, noting that the firewall is one of the "best application filtering firewalls on the market."

Press release:

< <http://www.net-security.org/text/press/968677494,15578,.shtml> >

SMARTCARD READER & FINGERPRINT SENSOR INTEGRATION - [13.09.2000]

Veridicom, Inc., the leader in fingerprint-based e-business authentication devices and services, unveiled a PC peripheral to combine a smartcard reader with a highly accurate Veridicom fingerprint sensor into a single device no larger than a computer mouse. The compact Veridicom 5thSense Combo peripheral makes it convenient to use multi-factor authentication with a smartcard by replacing passwords and Personal Identification Numbers with simple "just-press-here" fingerprint authentication.

Press release:

< <http://www.net-security.org/text/press/968677552,80833,.shtml> >

WANT TO BUY ENCRYPTION.COM? - [13.09.2000]

DomainMinds.com, LLC, a California-based domain name brokerage, announced that it is handling the auction of the highly coveted encryption.com domain name. "We are very excited to have the opportunity to offer this domain for sale," said DomainMinds.com, LLC president and CEO Blair Cummins. "With growing concern over Internet privacy and security, the encryption industry is showing rapid growth. The company that acquires the encryption.com domain will gain a strong advantage in what looks to be a highly competitive market. This truly is a powerful brand asset."

Press release:

< <http://www.net-security.org/text/press/968803014,51043,.shtml> >

ALLADIN LAUNCHES ESAFE GATEWAY 3.0 - [13.09.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, launched eSafe Gateway 3.0, the first and only all-in-one proactive content security solution that protects corporate networks and users from known and unknown attacks, before they get to users' personal computers. Using new patent-pending NitroInspection technology, eSafe Gateway 3.0 allows for an uninterrupted flow of secure Internet content without the sacrifice in

performance that occurs with competitive solutions.

Press release:

< <http://www.net-security.org/text/press/968803081,53343,.shtml> >

NEW CLASSES FOR HACKING AND SECURING WINDOWS - [13.09.2000]

Foundstone Inc., the premier computer security training and consulting company, announced a new series of computer security classes, Ultimate NT/2000 Security: Hands On. The classes will teach how to combat security threats to Windows NT and Windows 2000 systems. The first class will be held in New York City on October 10th, with an additional class scheduled for New York in December. Participants will learn security techniques from a hacker's perspective, assessing architectural vulnerabilities and deploying countermeasures. Topics covered will include "Password Cracking," "Buffer Overflow Attacks," "Gaining Command-Line Access," and "Registry Manipulation."

Press release:

< <http://www.net-security.org/text/press/968803183,88077,.shtml> >

SYBARI ENTERS BUSINESS SOLUTIONS FOR EXCHANGE - [13.09.2000]

Sybari Software, Inc., the premier antivirus and security specialist for groupware solutions today announced their acceptance into Compaq's Business Solutions for Exchange Program. Entry into Compaq's alliance of leading technology company's is yet another aggressive move by Sybari to further extend their reach to the Microsoft Exchange community with their award-winning antivirus and security solution, Antigen.

Press release:

< <http://www.net-security.org/text/press/968803443,21714,.shtml> >

NETGUARD FIREWALL FOR JUST \$9,95 - [13.09.2000]

Businesses and corporations operating on Windows NT can now protect themselves from hackers, computer hijackers and internal bandwidth hogs thanks to a free firewall from NetGuard, Inc., a leading provider of enterprise class network security, privacy and management solutions.

Press release:

< <http://www.net-security.org/text/press/968803558,24065,.shtml> >

CYLINK'S PRIVATEWIRE SECURES FINANCIAL TRANSACTIONS - [14.09.2000]

Cylink Corporation, a leading provider of secure e-business solutions, announced that Ball State Federal Credit Union has reached the 1,000-member milestone in sign-ups for secure access to financial information over the Internet using Cylink PrivateWire authentication and encryption technology.

Press release:

< <http://www.net-security.org/text/press/968887674,50364,.shtml> >

TREND MICRO PROTECTS SYDNEY GAMES ORGANISERS - [14.09.2000]

Trend Micro Inc. announced that it has doubled its response team ahead of the Olympic Games' opening this Friday, in readiness to support such customers as the Sydney Organising Committee of the Olympic Games, Stadium Australia, the Sydney Opera House, New South Wales Police, Sydney Airport and Telstra during the hectic games period. In addition, Trend Micro has teamed up with Telstra to provide remotely-managed antivirus services to Stadium Australia, making it the first site in Australia to receive 24x7 "live" antivirus monitoring for the duration of the games.

Press release:

< <http://www.net-security.org/text/press/968887867,97472,.shtml> >

SECUDE TO INTRODUCE IDENTRUS SECURITY SOLUTIONS - [14.09.2000]

German software supplier SECUDE GmbH is one of the first companies to offer security solutions complying with the Identrus standards for a global public key infrastructure, a critical step in enabling secure electronic financial transactions to take place over the Internet. Identrus is an initiative of leading international banks to establish binding standards for secure online transactions. Identrus standards ensure that the mutual electronic authentication of transactions creates an acknowledged reliability between banks and their business partners.

Press release:

< <http://www.net-security.org/text/press/968888022,35898,.shtml> >

PSA SECURITY NETWORKS RECOMMENDS MOTOROLA FLEXPASS - [14.09.2000]

ASIS Motorola announced that PSA Security Network, a large international electronic security systems company, now recommends Motorola FlexPass RFID security products for all new installations of proximity security and access control systems. "We see Motorola putting the kind of energy into customer service that produces and sustains real results, and we like that," says Jim Hawver, vice-president of sales and marketing at PSA Security Network.

Press release:

< <http://www.net-security.org/text/press/968888158,76071,.shtml> >

HIGH-LEVEL SECURITY SOLUTIONS FOR RACKSPACE - [14.09.2000]

Rackspace Managed Hosting, a leading provider of managed Internet hosting services, announced the launch of its new security offerings and managed security services, which provide Rackspace customers with a wide range of high-level security solutions. Round-the-clock support staff will be available both at Rackspace and through a partnership with ManagedFirewall.com to

resolve security issues on demand.

Press release:

< <http://www.net-security.org/text/press/968896285,6915,.shtml> >

CYLINK NETHAWK VPN "BEST BUY" IN SC MAGAZINE - [15.09.2000]

E-business security solutions provider Cylink Corporation announced that its NetHawk VPN, a high-performance virtual private network appliance for establishing secure Internet communications, has been named "Best Buy" in the September issue of SC Magazine. The information security magazine's product review lauded NetHawk for "its exceptional speed and reliability" and the VPN's PrivaCy Manager, a policy-based management application. "Once the device manager is installed, it is extremely scaleable; you simply plug in new boxes as and when you need them, which is perfect for any growing business," the review said.

Press release:

< <http://www.net-security.org/text/press/969017587,37286,.shtml> >

Featured articles

All articles are located at:

<http://www.net-security.org/text/articles>

Articles can be contributed to staff@net-security.org

Listed below are some of the recently added articles.

ISSUES: THE SECURITY OF ELECTRONIC BANKING, LEGACY OF THE COW by Thejian

The article starts with the Dutch television show that exposed the Dutch banking organisation ABN AMRO's HomeNet program as being insecure. Computer science students had found a way to trick this electronic banking system into redirecting a user's bank transfers to a different account. As could have been expected, press and consumer organisations fell en masse for the possibilities the idea of "hackers" snooping around in your bank account presented. And it doesn't stop there...

Article:

< <http://www.net-security.org/text/articles/thejian/legacy.shtml> >

VIRUS SCANNER INADEQUACIES WITH NTFS by Chris Brenton

While the existence of data streams within the NT file system (NTFS) has been known for many years (Microsoft has released quite a bit of info on alternate

streams), virus vendors have not taken steps to adequately check this area of the file system. This deficiency can be leveraged in order to hide malicious code or even cause the virus scanner itself to destroy critical system files.

Paper:

< <http://www.net-security.org/text/articles/viruses/ntfs.shtml> >

A DIFFERENT LANGUAGE ACROSS THE BORDER by Hyper Viper

In this article Hyper Viper explains how bi-lingual servers speaking different protocols to different networks can add security to your Internet exposed nodes.

Article:

< <http://www.net-security.org/text/articles/language.shtml> >

BUILDING A BASTION HOST USING HP-UX 11 by Kevin Steves

A bastion host is a computer system that is exposed to attack, and may be a critical component in a network security system. Special attention must be paid to these highly fortified hosts, both during initial construction and ongoing operation. This paper presents a methodology for building a bastion host using HP-UX 11. While the principles and procedures can be applied to other HP-UX versions as well as other Unix variants, the focus is on HP-UX 11.

Paper:

< <http://www.net-security.org/text/articles/index-download.shtml#HP-UX> >

NETWORK INTRUSION DETECTION OF THIRD PARTY EFFECTS by Richard Bejtlich

The main goal of this paper is to familiarize the reader with reactions and responses from innocent victims, who may be subject to reconnaissance or denial of service. If a perpetrator spoofs your address space you may see unsolicited traffic from an innocent second party.

Paper:

< <http://www.net-security.org/text/articles/index-download.shtml#NID> >

PROPHYLAXIS OF COMPUTER INFECTION by Kaspersky Lab

One of the major methods of fighting computer viruses, like in medical science, is timely prophylaxis or preventive measures. Computer preventive measures suggest following a small set of rules, allowing to lower considerably the possibility of virus infection and data loss. To define the main rules of computer hygiene, it is necessary to find out the main ways of virus intrusion into computer and computer network.

Article:

< <http://www.net-security.org/text/articles/viruses/infection.shtml> >

FORMAT STRING ATTACKS by Tim Newsham

The cause and implications of format string vulnerabilities are discussed. Practical examples are given to illustrate the principles presented.

Article:

< <http://www.net-security.org/text/articles/string.shtml> >

KASPERSKY LAB REFUTES ACCUSATIONS ABOUT THE SPREADING OF "VIRUS HYSTERIA"

Given the latest events, Kaspersky Lab would like to once again confirm its position regarding the danger present in the NTFS alternate data streams. Furthermore, we state that by continuing to ignore the problem and not taking similar steps-steps that Kaspersky Lab has already taken and continues to take-to bring their anti-virus product up to contemporary standards, the aforementioned competitor anti-virus companies are neglecting their users' anti-virus security.

Article:

< <http://www.net-security.org/text/articles/viruses/hysteria.shtml> >

COMPUTER SECURITY WEAKNESSES PERSIST AT THE VETERANS HEALTH ADMINISTRATION

In September 1998, the General Accounting Office reported that computer security weaknesses placed critical VA operations, including health care delivery, at risk of misuse and disruption. Since then, VA's New Mexico and North Texas health care systems have corrected most of the specific computer security weaknesses that were identified in 1998. However, serious computer security problems persist throughout VHA and the department.

Paper:

< <http://www.net-security.org/text/articles/index-download.shtml#CSW> >

QUANTUM CRYPTOGRAPHY by Caboom

This tutorial will give you a basic idea about quantum cryptography.

Paper:

< <http://www.net-security.org/text/articles/index-download.shtml#Quantum> >

MAIL ABUSE PREVENTION ORGANIZATION STANDS UP TO GIANT HARRIS INTERACTIVE

Mail Abuse Prevention System, the Redwood City based anti-spam organization, says that it will vigorously defend the law suit filed by online market research giant Harris Interactive Inc. Harris has sued Microsoft, and AOL, naming MAPS as a co-defendant, in an effort to force Microsoft and AOL to accept unsolicited bulk commercial email, also known as "spam", from Harris. MAPS maintains several

databases which companies such as Microsoft's Hotmail use to help them manage the Internet email traffic which crosses their networks. We have a copy of the complaint.

Complaint:

< <http://www.net-security.org/text/articles/index-download.shtml#MAPS> >

Featured books

The HNS bookstore is located at:
<http://net-security.org/various/bookstore>

Suggestions for books to be included into our bookstore can be sent to staff@net-security.org

TOP SECRET INTRANET: HOW U.S. INTELLIGENCE BUILT INTELINK
THE WORLD'S LARGEST, MOST SECURE NETWORK

Using the example of "Intelink", the classified worldwide Intranet for the intelligence community, this book is one of the first on current intelligence operations written by an "insider". The CD-ROM includes sample Intelink software demos relating to collaboration tools, security products, and other applications.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130808989/netsecurity> >

BLACK BELT WEB PROGRAMMING METHODS; SERVERS, SECURITY, DATABASES AND SITES

Use this book to build a robust infrastructure for powerful Web sites. Master programmers who write for Web Techniques, Dr. Dobb's Journal, Interactivity, Data Base Management Systems, Network, and Software Development have joined forces to tackle the latest round of web programming puzzles for you. Learn airtight security procedures and hypertext transaction designs. Build databases that are easy to use. Whether you need to create distributed objects or automate Web site maintenance, these seasoned programmers explain how to do it right, and they give you the code to do the job. The companion code disk includes detailed, reusable code for each of the applications presented. Programming languages include C/C++ and Java.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0879304979/netsecurity> >

ENCYCLOPEDIA OF DISASTER RECOVERY, SECURITY & RISK MANAGEMENT

The Encyclopedia of Disaster Recovery, Risk Management & Security is a 300+

page spiral bound manual, which provides over 2,000 pieces of research on the subjects of disaster recovery, risk management and security. The Encyclopedia is a comprehensive reference guide organized by easy to follow icons allowing quick navigation to areas of specific interest. The Encyclopedia draws on Mr. Schreiders 20+ years of experience in an A to Z presentation of industry research, risk management guidelines, recovery planning tips and techniques, security safeguards, and terminology. Disaster Recovery Planners, Risk Managers, and Security Administrators will all equally benefit from this invaluable storehouse of knowledge.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0966272900/netsecurity> >

BUILDING LINUX CLUSTERS

This book discusses complex modeling, virtual world creation, and image generation; shows readers how to choose hardware; and explains cluster topologies. As the author notes, Linux clusters regularly make the list of the world's top 500 supercomputers. Not bad for a free system. Of course, running your own cluster isn't trivial, but the book shows how straightforward it can be for basic clusters, and how far clusters can be extended. The book covers the all-important intermachine-communications issues in exhaustive depth. Setting up the hardware can be relatively straightforward as is the software installation. The tutorial uses Red Hat's 6 Linux distribution--it's supplied with the book--and adds all the clustering software and tools.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1565926250/netsecurity> >

CORBA SECURITY: AN INTRODUCTION TO SAFE COMPUTING WITH OBJECTS

The CORBA security specification adopted by the Object Management Group (OMG) represents a major step forward in making object technology suitable for business application development. The specification document, however, is long, detailed, and complex; it is a time-consuming task for software developers to make their way through it, and it is inaccessible to CIOs and other technical managers who need to understand object security and its impact on their organizations.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201325659/netsecurity> >

Security Software

All programs are located at:
<http://net-security.org/various/software>

FIRE-WALLER (LINUX)

Fire-Waller reads your syslog against packet filter rows and creates HTML output of the found rows. All addresses in logfiles are checked against a nameserver and protocols/services are converted from numeric values to text.

Link:

< <http://net-security.org/various/software/968030527,29733,.shtml> >

NETWORK SECURITY ANALYSIS TOOL (LINUX)

NSAT is a fast, stable bulk security scanner designed to audit remote network services and check for versions, security problems, gather information about the servers and the machine, and much more. Unlike many other auditing tools, it can collect information about services independently of vulnerabilities, which makes it less dependent on frequent updates as new vulnerabilities are found.

Link:

< <http://net-security.org/various/software/968030615,24271,.shtml> >

WINDOWS 2000 IIS 5.0 HOTFIX CHECKING TOOL

The HFCheck tool allows IIS5.0 administrators to ensure that their servers are up to date on all security patches. The tool can be run continuously or periodically, against the local machine or a remote one, using either a database on the MS web site or a locally-hosted copy. When the tool finds a patch that hasn't been installed, it can display or dialogue or write a warning to the event log.

Link:

< <http://net-security.org/various/software/968181513,8218,.shtml> >

WINZAPPER FOR WINDOWS NT 4.0 AND WIN 2K

WinZapper can only be used from an Administrators account, thus this has nothing to do with any new security vulnerabilities in Windows NT / 2000. After an attacker has gained Administrators access to your system, you simply cannot trust your security log! And as always, remember that attacker having that kind of access can do anything to your system!

Link:

< <http://net-security.org/various/software/968284983,30844,.shtml> >

SCANSSH (LINUX)

Scanssh scans a list of addresses and networks for running SSH servers and their version numbers. scanssh supports random selection of IP addresses from large network ranges and is useful for gathering statistics on the deployment of

SSH servers in a company or the Internet as whole.

Link:

< <http://net-security.org/various/software/968334220,65880,.shtml> >

ANTIVIRUS FOR PALM OS BETA

Symantec AntiVirus for Palm OS is a Palm application that scans for and detects viruses in all Palm OS-compatible devices. Symantec AntiVirus for Palm OS ensures security for your data by running on-demand scans that detect and remove viruses directly on your handheld device, protecting data even between synchronizations.

Mac users:

< <http://net-security.org/various/software/968461705,78724,.shtml> >

PC users:

< <http://net-security.org/various/software/968461805,3997,.shtml> >

VSE MY PRIVACY 1.2.1 (MAC)

VSE My Privacy is data security software that allows you to store and organize your confidential data in a safe place. It uses a military-strength, 448-bit encryption algorithm designed to be uncrackable. The application is designed to store bank account information, credit card numbers, Web site passwords, telephone numbers, private addresses, email account passwords, PINs, keys for unlocking software, membership numbers, and other confidential data in a simple and easy-to-use database.

Link:

< <http://net-security.org/various/software/968461997,17766,.shtml> >

Defaced archives

[10.09.2000] - Ohio State Department of Commerce

Original: <http://www.com.state.oh.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/10/www.com.state.oh.us/>

[10.09.2000] - Government of Guam

Original: <http://www.admin.gov.gu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/10/www.admin.gov.gu/>

[10.09.2000] - LegoLand Windsor

Original: <http://www.legoland.co.uk/>

Defaced: <http://www.net-security.org/misc/sites/www.legoland.co.uk/>

[10.09.2000] - Soccer Central USA

Original: <http://www.soccercentralusa.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/10/www.soccercentralusa..com/>

[10.09.2000] - North Carolina State Department of Commerce

Original: <http://www.commerce.state.nc.us/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/10/www.commerce.state.nc.us/>

[11.09.2000] - MIT Department of Chemical Engineering

Original: <http://montoresa.mit.edu/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/11/montoresa.mit.edu/>

[11.09.2000] - Ryan D Williams MIT Web site

Original: <http://rdw.mit.edu/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/11/rdw.mit.edu/>

[11.09.2000] - First Domain Name Company

Original: <http://www.firstdomainnamecompany.com/>
Defaced:
<http://www.attrition.org/mirror/attrition/2000/09/11/www.firstdomainnamecompany.com/>

[11.09.2000] - World Peace Collection

Original: <http://www.worldpeacecollection.com/>
Defaced:
<http://www.attrition.org/mirror/attrition/2000/09/11/www.worldpeacecollection.com/>

[11.09.2000] - Elite Crew

Original: <http://www.elitecrew.nu/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/11/www.elitecrew.nu/>

[12.09.2000] - GhostMail

Original: <http://www.ghostmail.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/12/www.ghostmail.com/>

[12.09.2000] - New American Leasing & Financing

Original: <http://www.newamericanleasing.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/12/www.newamericanleasing.com/>

[12.09.2000] - r00tabega

Original: <http://www.r00tabega.org/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/12/www.r00tabega.org/>

[12.09.2000] - #2 Organization of the Petroleum Exporting Countries

Original: <http://www.opec.org/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/12/www.opec.org/>

[13.09.2000] - Pennsylvania State Government

Original: <http://www.dgs.state.pa.us/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/13/www.dgs.state.pa.us/>

[13.09.2000] - Incra/Instituto Nacional de Colon e Ref. Acgraria

Original: <http://www.nead.gov.br/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/13/www.nead.gov.br/>

[14.09.2000] - Citizen's Scholarship Foundation

Original: <http://www.csfa.org/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/14/www.csfa.org/>

[15.09.2000] - Spamlaws.com
Original: <http://www.spamlaws.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/15/www.spamlaws.com/>

[15.09.2000] - National Highway Traffic Safety Administration
Original: <http://www.nhtsa.dot.gov/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/15/www.nhtsa.dot.gov/>

[16.09.2000] - American Osteopathic Association
Original: <http://www.aoa-net.org/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/16/www.aoa-net.org/>

[16.09.2000] - Technosoft HK Ltd
Original: <http://www.technosofthk.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/16/www.technosofthk.com/>

[17.09.2000] - Internet Shinmun Co.,Ltd.
Original: <http://www.2000korea.co.kr/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/17/www.2000korea.co.kr/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org
<http://net-security.org>